arXiv:1202.6343v1 [math.NT] 28 Feb 2012

DERIVED P-ADIC HEIGHTS AND P-ADIC L-FUNCTIONS

BENJAMIN HOWARD

Abstract. If E is an elliptic curve defined over a number field and p is a prime of good ordinary reduction for E, a theorem of Rubin [14], Thm. 1, relates the p-adic height pairing on the p-power Selmer group of E to the first derivative of a cohomologically defined p-adic L-function attached to E. Bertolini and Darmon [3] have defined a sequence of "derived" p-adic heights. In this paper we give an alternative definition of the p-adic height pairing and prove a generalization of Rubin's result, relating the derived heights to higher derivatives of p-adic L-functions. We also relate degeneracies in the derived heights to the failure of the Selmer group of E over a $\mathbf{Z}_p$-extension to be "semi-simple" as an Iwasawa module, generalizing results of Perrin-Riou [12].

0. Introduction and Notation

Fix forever a rational prime $p > 2$. By a coefficient ring we mean a commutative ring which is complete, Noetherian, and local with residue field of characteristic p. Fix a finite set of places Σ of a number field F containing all archimedean places and all primes above p, and let $G_\Sigma = \mathrm{Gal}(F_\Sigma/F)$ where F_Σ is the maximal extension of F unramified outside of Σ. For any coefficient ring R, denote by $\mathbf{Mod}_\Sigma(R)$ the category of free R-modules of finite type equipped with continuous, R-linear actions of G_Σ. The notation $M(k)$ for any G_Σ-module M means Tate twist, as usual.

Throughout this article we work with a fixed coefficient ring $\mathcal{O}$, which is assumed to be topologically discrete (at least until Section 4), for example $\mathcal{O} = \mathbf{Z}/p^k\mathbf{Z}$. With F as above let F_∞/F be a $\mathbf{Z}_p$-extension. If $F_n \subset F_\infty$ is the unique subfield with $[F_n : F] = p^n$, we define

$$\Gamma_n = \mathrm{Gal}(F_n/F) \qquad \Gamma = \mathrm{Gal}(F_\infty/F) \qquad \Lambda_n = \mathcal{O}[\Gamma_n] \qquad \Lambda = \mathcal{O}[[\Gamma]],$$

and denote by J the augmentation ideal of Λ. Let $\gamma \in \Gamma$ be a topological generator and denote by ι the involution of Λ induced by $\gamma \mapsto \gamma^{-1}$. We will also view ι as a functor $M \mapsto M^\iota$ from the category of Λ-modules to itself, where the underlying group of M^ι is the same as that of M but with Λ acting through $\Lambda \xrightarrow{\iota} \Lambda \to \mathrm{End}_{\mathcal{O}}(M)$.

In Section 1 we consider two objects S, T of $\mathbf{Mod}_\Sigma(\mathcal{O})$ which are assumed to be in Cartier duality: i.e. we assume that there exists a perfect $\mathcal{O}$-bilinear, G_Σ-equivariant pairing $S \times T \to \mathcal{O}(1)$. For such objects we define generalized Selmer groups

$$H^1_{\mathcal{F}}(F, S_\infty) \subset \varinjlim H^1(F_n, S) \qquad H^1_{\mathcal{G}}(F, T_\infty) \subset \varinjlim H^1(F_n, T)$$

and show that there is a canonical (up to sign) height pairing

$$H^1_{\mathcal{F}}(F, S_\infty) \times H^1_{\mathcal{G}}(F, T_\infty) \to J/J^2$$

2000 *Mathematics Subject Classification.* 11G05, 11R23.

This research was partially conducted by the author for the Clay Mathematics Institute.

whose kernels on either side are the submodules of *universal norms* in the sense of Definition 1.3.

We continue to work in great generality in Section 2, using the construction of Section 1 to define derived height pairings similar to those of Bertolini and Darmon. A theorem of Rubin [14], Thm. 1, relates the p-adic height pairing to the special values of the first derivatives of certain (cohomologically defined) p-adic L-functions, and we prove similar formulas relating the derived heights to special values of higher derivatives.

In Section 3 we consider the special case where S and T arise from torsion points on an abelian variety with good, ordinary reduction at primes of F above p, and show that our Selmer groups agree with the usual ones (up to a controlled error).

In Section 4 we continue to work with torsion points on an abelian variety A, and explain how degeneracies in the derived heights are reflected in the structure of the Selmer group of A over F_∞ as an Iwasawa module, generalizing work of Perrin-Riou [12].

The reader is encouraged to begin by reading the results of Section 4, in particular Theorems 4.2 and 4.5, and Corollary 4.3.

1. Construction of the p-adic height pairing

We wish to work with a very general notion of Selmer group, borrowing some notation and conventions from [9].

Definition 1.1. Suppose R is a coefficient ring and M is topological R-module equipped with a continuous R-linear action of G_Σ. A *Selmer structure*, $\mathcal{F}$, on M is a choice of R-submodule

$$H^1_{\mathcal{F}}(F_v, M) \subset H^1(F_v, M)$$

for every $v \in \Sigma$. Given a Selmer structure, the associated *Selmer module* $H^1_{\mathcal{F}}(F, M)$ is defined to be the kernel of

$$H^1(G_\Sigma, M) \ \to \ \bigoplus_{v \in \Sigma} H^1(F_v, M)/H^1_{\mathcal{F}}(F_v, M).$$

If we are given a Selmer structure $\mathcal{F}$ on M and a surjection $M \ \to \ M'$, we obtain a Selmer structure on M' (still denoted $\mathcal{F}$) by taking the local condition at any $v \in \Sigma$ to be the image of

$$H^1_{\mathcal{F}}(F_v, M) \ \to \ H^1(F_v, M').$$

If instead we are given an injection $M' \ \to \ M$ then we define a Selmer structure on M' by taking the preimage of $H^1_{\mathcal{F}}(F_v, M)$ under

$$H^1(F_v, M') \ \to \ H^1(F_v, M).$$

We will refer to this as *propagation* of Selmer structures.

If (T, π) belongs to $\mathbf{Mod}_\Sigma(\mathcal{O})$, then induction from $\mathrm{Gal}(F_\Sigma/F_n)$ to $\mathrm{Gal}(F_\Sigma/F)$ defines a module (T_n, π_n) in $\mathbf{Mod}_\Sigma(\Lambda_n)$. Explicitly,

$$T_n = \{f : G_\Sigma \ \to \ T \mid f(gx) = \pi(g)f(x) \ \forall g \in \mathrm{Gal}(F_\Sigma/F_n)\}.$$

Here G_Σ acts by $(\pi_n(g)f)(x) = f(xg)$ and Λ_n acts by $(\gamma f)(x) = \pi(\tilde{\gamma})f(\tilde{\gamma}^{-1}x)$ where $\tilde{\gamma}$ is any lift of $\gamma \in \Gamma_n$ to G_Σ. Define

$$T_\infty = \varinjlim T_n \qquad T_{\mathrm{Iw}} = \varprojlim T_n$$

where the direct limit is with respect to the natural inclusions (restriction) and the inverse limit is with respect to the norm operators in Λ_n (corestriction). Let $\mathrm{ev} : T_\infty \to T$ be evaluation at the identity element of G_Σ. By Shapiro's lemma the composition

$$H^i(F, T_\infty) \xrightarrow{\text{res}} H^i(F_\infty, T_\infty) \xrightarrow{\text{ev}} H^i(F_\infty, T)$$

is an isomorphism, and similarly we have

$$H^i(F, T_{\mathrm{Iw}}) \cong \varprojlim H^i(F_n, T).$$

An element $\lambda \in \Lambda$ is said to be *distinguished* if $\lambda \notin \mathfrak{m}\Lambda$, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$.

Lemma 1.2. *If g_n is any sequence of elements of Λ which converges to zero and $f \in \Lambda$ is distinguished, then $f \mid g_n$ for $n \gg 0$.*

Proof. Identify Λ with a power series ring. The map taking $\lambda \in \Lambda$ to its remainder upon division by f is continuous, and so if we write $g_n = q_n f + r_n$ with degree of r_n less than that of f, we have $r_n \to 0$ with the r_n running through a discrete set (recall $\mathcal{O}$ is assumed discrete). □

If we fix a topological generator $\gamma \in \Gamma$ and let $g_n = \frac{\gamma^{p^n}-1}{\gamma-1}$ be the norm element in Λ_n, the above lemma shows that $m \in M$ is divisible by every distinguished $f \in \Lambda$ if and only if $m \in g_n M$ for every n. This motivates the following

Definition 1.3. If M is a Λ-module, we say that $m \in M$ is a *universal norm* if $m \in fM$ for every distinguished $f \in \Lambda$.

We denote by $\omega_{\mathrm{taut}} : G_\Sigma \to \Gamma \to \Lambda^\times$ the tautological character, and let $\Lambda\{k\}$ denote the ring Λ, viewed as a module over itself, on which G_Σ acts through ω_{taut}^k. The unadorned symbol Λ is always interpreted as $\Lambda\{0\}$, i.e. with trivial Galois action. For any object M on which Λ and G_Σ act we let $M\{k\} = M \otimes_\Lambda \Lambda\{k\}$, and we regard the underlying Λ-modules of M and $M\{k\}$ as being identified via $m \mapsto m \otimes 1$.

Lemma 1.4. *For $f \in T_n$ and $\gamma \in \Gamma_n$, set $\mu_f(\gamma) = \mathrm{ev}(\gamma^{-1} f) \in T$. The map $f \mapsto \sum_\gamma \mu_f(\gamma) \otimes \gamma$ defines an isomorphism in $\mathbf{Mod}_\Sigma(\Lambda_n)$*

$$T_n \cong T \otimes_{\mathcal{O}} \Lambda_n\{-1\}.$$

In the limit this defines an isomorphism $T_{\mathrm{Iw}} \cong T \otimes_{\mathcal{O}} \Lambda\{-1\}$.

Proof. This amounts to verifying the relations

$$\mu_{\gamma_0 f}(\gamma) = \mu_f(\gamma_0^{-1}\gamma) \qquad \mu_{\pi_n(g) f}(\gamma) = \pi(g)\big(\mu_f(\omega_{\mathrm{taut}}(g)\gamma)\big)$$

which are elementary. □

Let K denote the ring obtained by localizing Λ at the prime generated by the maximal ideal of $\mathcal{O}$, i.e. inverting all distinguished elements. Applying Lemma 1.2 one may easily check that K is noncanonically isomorphic to the ring of Laurent series with non-essential singularities in one variable over $\mathcal{O}$. Define P (the module of poles) by exactness of the sequence

$$0 \to \Lambda \to K \to P \to 0.$$

For any T in $\mathbf{Mod}_\Sigma(\mathcal{O})$ we tensor the above sequence (over Λ) with T_{Iw} to obtain

$$0 \ \to \ T_{\mathrm{Iw}} \ \to \ T_K \ \to \ T_P \ \to \ 0.$$

By Lemma 1.4 there are canonical identifications of Λ-modules and G_Σ-modules $\mathcal{O}_{\mathrm{Iw}} \cong \Lambda\{-1\}$, $\mathcal{O}_K \cong K\{-1\}$, and $\mathcal{O}_P \cong P\{-1\}$.

Lemma 1.5. *A choice of topological generator of Γ determines an isomorphism*

$$T_P \cong T_\infty.$$

If the map associated to the generator γ is denoted η_γ and $u \in \mathbf{Z}_p^\times$ then $\eta_{\gamma^u} = u \cdot \eta_\gamma$.

Proof. The map η_γ is described as follows. Any element of $T_P[\gamma^{p^n} - 1]$ may be written as $\tau \otimes (\gamma^{p^n} - 1)^{-1}$ with $\tau \in T_{\mathrm{Iw}}$. Such an element is sent by η_γ to the image of τ in $T_n \cong T_\infty[\gamma^{p^n} - 1]$. The relation between η_γ and η_{γ^u} follows from

$$\frac{\gamma^{up^n} - 1}{\gamma^{p^n} - 1} \equiv u \pmod{(\gamma^{p^n} - 1)\Lambda}.$$

□

Lemma 1.6. *Suppose $e : S \times T \ \to \ \mathcal{O}(1)$ is an $\mathcal{O}$-bilinear, G_Σ-equivariant, perfect pairing of objects in $\mathbf{Mod}_\Sigma(\mathcal{O})$. There is an induced G_Σ-equivariant and perfect pairing*

$$e_n : S_n \times T_n \ \to \ \Lambda_n(1)$$

which satisfies

$$e_n(\lambda s, t) = \lambda e_n(s,t) = e_n(s, \lambda^\iota t).$$

One may pass to the limit and then tensor with K to obtain perfect pairings

$$e_{\mathrm{Iw}} : S_{\mathrm{Iw}} \times T_{\mathrm{Iw}} \ \to \ \Lambda(1) \qquad e_K : S_K \times T_K \ \to \ K(1).$$

If $S = T$ and the pairing on $S \times T$ is symmetric (resp. alternating) then the induced pairings satisfy $e_\bullet(s,t) = e_\bullet(t,s)^\iota$ (resp. $e_\bullet(s,t) = -e_\bullet(t,s)^\iota$).

Proof. Using the identifications of Lemma 1.4, the pairing is defined by $e_n(s,t) = \sum_{\gamma \in \Gamma_n} \mu(\gamma) \otimes \gamma$ where $\mu(\gamma) = \sum_{x \in \Gamma_n} e(\mu_s(x), \mu_t(x\gamma^{-1}))$. It is elementary to check that the stated properties hold. □

Lemma 1.7. *Let T be an object of $\mathbf{Mod}_\Sigma(\mathcal{O})$, and let v be a prime of F not dividing p. The map*

$$H^1_{\mathrm{unr}}(F_v, T_K) \ \to \ H^1_{\mathrm{unr}}(F_v, T_P)$$

is surjective. If v is finitely decomposed in F_∞, then $H^1_{\mathrm{unr}}(F_v, T_P) = 0$.

Proof. Let $\mathcal{I} \subset \mathrm{Gal}(\bar{F}_v/F_v)$ be the inertia group of v. Since $T_K = T \otimes_{\mathbf{Z}_p} K\{-1\}$ and the restriction of ω_{taut} to $\mathcal{I}$ is trivial, $(T_K)^{\mathcal{I}} = T^{\mathcal{I}} \otimes K$. Similarly, $(T_P)^{\mathcal{I}} = T^{\mathcal{I}} \otimes P$, and so $(T_K)^{\mathcal{I}}$ surjects onto $(T_P)^{\mathcal{I}}$. Using the fact that $\mathrm{Gal}(F_v^{\mathrm{unr}}/F_v)$ has cohomological dimension one we deduce that the map

$$H^1(F_v^{\mathrm{unr}}/F_v, (T_K)^{\mathcal{I}}) \ \to \ H^1(F_v^{\mathrm{unr}}/F_v, (T_P)^{\mathcal{I}})$$

is surjective, proving the first claim.

If v is finitely decomposed in F_∞, then Lemma 1.5 and Shapiro's lemma allow us to identify

$$H^1_{\mathrm{unr}}(F_v, T_P) \cong H^1_{\mathrm{unr}}(F_v, T_\infty) \cong \bigoplus_w H^1_{\mathrm{unr}}(F_{\infty,w}, T)$$

where the sum is over places of F_∞ above v. The pro-p-part of $\mathrm{Gal}(F_v^{\mathrm{unr}}/F_{\infty,w})$ is trivial, and so the right hand side is zero. □

The construction of the pairing of the following theorem, as well as the verification of its properties, is a modification of the construction of the Cassels-Tate pairing as described in [6].

Theorem 1.8. *Suppose S and T are objects in $\mathbf{Mod}_\Sigma(\mathcal{O})$ and that there is a perfect G_Σ-equivariant pairing $S \times T \to \mathcal{O}(1)$. Suppose further that we are given Selmer structures $\mathcal{F}$ and $\mathcal{G}$ on S_K and T_K, respectively, which are everywhere exact orthogonal complements under the pairing*

$$S_K \times T_K \to K(1).$$

Then there is a canonical pairing

$$[\ ,\ ] : H^1_{\mathcal{F}}(F, S_P) \times H^1_{\mathcal{G}}(F, T_P) \to P$$

whose kernels on the left and right are the images of $H^1_{\mathcal{F}}(F, S_K)$ and $H^1_{\mathcal{G}}(F, T_K)$, and these images are exactly the submodules of universal norms. This pairing satisfies $[\lambda s, t] = \lambda[s, t] = [s, \lambda^\iota t]$. If $S = T$, $\mathcal{F} = \mathcal{G}$, and the pairing on $T \times T$ is symmetric (resp. alternating) then we also have $[s, t] = [t, s]^\iota$ (resp. $[s, t] = -[t, s]^\iota$).

Proof. Given cocycles s and t representing classes in $H^1_{\mathcal{F}}(F, S_P)$ and $H^1_{\mathcal{G}}(F, T_P)$, respectively, choose cochains

$$\tilde{s} \in C^1(G_\Sigma, S_K) \qquad\qquad \tilde{t} \in C^1(G_\Sigma, T_K)$$

whose images under the maps induced by $S_K \to S_P$ and $T_K \to T_P$ are s and t. By the definition of propagation of Selmer structures, there are exact sequences

$$\begin{aligned} H^1_{\mathcal{F}}(F_v, S_{\mathrm{Iw}}) &\to H^1_{\mathcal{F}}(F_v, S_K) \to H^1_{\mathcal{F}}(F_v, S_P) \to 0 \\ H^1_{\mathcal{G}}(F_v, T_{\mathrm{Iw}}) &\to H^1_{\mathcal{G}}(F_v, T_K) \to H^1_{\mathcal{G}}(F_v, T_P) \to 0 \end{aligned} \tag{1}$$

at every $v \in \Sigma$, and so we may choose semi-local classes

$$\tilde{s}_\Sigma \in \bigoplus_{v \in \Sigma} H^1_{\mathcal{F}}(F_v, S_K) \qquad \tilde{t}_\Sigma \in \bigoplus_{v \in \Sigma} H^1_{\mathcal{G}}(F_v, T_K)$$

which reduce to the semi-localizations

$$\mathrm{loc}_\Sigma(s) \in \bigoplus_{v \in \Sigma} H^1_{\mathcal{F}}(F_v, S_P) \qquad \mathrm{loc}_\Sigma(t) \in \bigoplus_{v \in \Sigma} H^1_{\mathcal{G}}(F_v, T_P).$$

From the fact that s and t are cocycles it follows that the image of $d\tilde{s} \cup d\tilde{t}$ in $C^4(G_\Sigma, P(1))$ is trivial, and so also are the images of $d(d\tilde{s} \cup \tilde{t}) = d\tilde{s} \cup d\tilde{t} = d(\tilde{s} \cup d\tilde{t})$. Using $H^3(G_\Sigma, P(1)) = 0$ we may therefore choose $\epsilon_0, \epsilon_1 \in C^2(G_\Sigma, P(1))$ such that

$$d\epsilon_0 = d\tilde{s} \cup \tilde{t} \qquad\qquad d\epsilon_1 = \tilde{s} \cup d\tilde{t}$$

in $Z^3(G_\Sigma, P(1))$. Writing $\mathrm{inv}_\Sigma : \bigoplus_{v \in \Sigma} H^2(F_v, P(1)) \to P$ for the sum of the local invariants, we now define

$$[s, t] = \mathrm{inv}_\Sigma\big(\mathrm{loc}_\Sigma(\tilde{s}) \cup \tilde{t}_\Sigma - \mathrm{loc}_\Sigma(\epsilon_0)\big) = -\mathrm{inv}_\Sigma\big(\tilde{s}_\Sigma \cup \mathrm{loc}_\Sigma(\tilde{t}) + \mathrm{loc}_\Sigma(\epsilon_1)\big) \tag{2}$$

where the second equality follows from $(\mathrm{loc}_\Sigma(\tilde{s}) - \tilde{s}_\Sigma) \cup (\mathrm{loc}_\Sigma(\tilde{t}) - \tilde{t}_\Sigma) = 0$ in $\bigoplus_{v \in \Sigma} H^1(F_v, P(1))$ and the reciprocity law of class field theory. It is elementary to check that this is independent of the choices made (or see Flach's paper for essentially the same calculations). Furthermore, it is clear from the construction that the kernels on either side contain the images of $H^1_{\mathcal{F}}(F, S_K)$ and $H^1_{\mathcal{G}}(F, T_K)$.

For a Λ-module M, we write $M^\vee = \mathrm{Hom}_\Lambda(M^\iota, P)$. If M is a topological group on which G_Σ acts continuously we define

$$Ш^i(F,M) = \ker\bigl(H^i(G_\Sigma, M) \ \to \ \prod_{v\in\Sigma} H^i(F_v, M)\bigr).$$

The Poitou-Tate nine-term exact sequence provides a perfect pairing

$$Ш^2(F, S_{\mathrm{Iw}}) \times Ш^1(F, T_P) \ \to \ P$$

which defines the right vertical arrow in the exact and commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & H^1_{\mathcal{F}}(F,S_P)^0{}_{/K} & \longrightarrow & H^1_{\mathcal{F}}(F,S_P)_{/K} \longrightarrow Ш^2(F,S_{\mathrm{Iw}}) \\ & & & & \downarrow \qquad\qquad \downarrow \\ & & & & H^1_{\mathcal{G}}(F,T_P)^\vee \longrightarrow Ш^1(F,T_P)^\vee. \end{array}$$

Here $H^1_{\mathcal{F}}(F,S_P)^0$ denotes $H^1_{\mathcal{F}}(F,S_P)$ intersected with the image of $H^1(F,S_K)$ in $H^1(F,S_P)$ and the subscript $/K$ indicates quotient by the image of $H^1_{\mathcal{F}}(F,S_K)$ in $H^1_{\mathcal{F}}(F,S_P)$. The top row is extracted from the cohomology of

$$0 \ \to \ S_{\mathrm{Iw}} \ \to \ S_K \ \to \ S_P \ \to \ 0$$

using exactness of (1).

The left vertical arrow is induced by the pairing of the theorem, and a diagram chase shows that to check injectivity of this arrow it suffices to show that $H^1_{\mathcal{F}}(F,S_P)^0{}_{/K}$ injects into $H^1_{\mathcal{G}}(F,T_P)^\vee$. In other words, if $s \in H^1_{\mathcal{F}}(F,S_P)$ is in the kernel on the left then we are free to assume that $\tilde{s}$ is chosen to be a cocycle and that $\epsilon_0 = 0$. Then we have $\mathrm{inv}_\Sigma\bigl(\mathrm{loc}_\Sigma(\tilde{s}) \cup \tilde{t}_\Sigma\bigr) = 0$ for every $\tilde{t}_\Sigma \in \bigoplus_{v\in\Sigma} H^1_{\mathcal{G}}(F_v, T_K)$ whose image in $\bigoplus_{v\in\Sigma} H^1_{\mathcal{G}}(F_v,T_P)$ comes from a global $t \in H^1_{\mathcal{G}}(F,T_P)$. Denote by c the image of $\mathrm{loc}_\Sigma(\tilde{s})$ in $\bigoplus_{v\in\Sigma} H^1(F_v,S_K)/H^1_{\mathcal{F}}(F_v,S_K)$. It follows from the exactness of (1) that there is a class

$$d \in \bigoplus_{v\in\Sigma} H^1(F_v, S_{\mathrm{Iw}})/H^1_{\mathcal{F}}(F_v, S_{\mathrm{Iw}})$$

whose image in $\bigoplus_{v\in\Sigma} H^1(F_v,S_K)/H^1_{\mathcal{F}}(F_v,S_K)$ is equal to c. Then

$$\begin{aligned} \mathrm{inv}_\Sigma(d \cup \mathrm{loc}_\Sigma(t)) &= \mathrm{inv}_\Sigma(c \cup \tilde{t}_\Sigma) \\ &= \mathrm{inv}_\Sigma(\mathrm{loc}_\Sigma(\tilde{s}) \cup \tilde{t}_\Sigma) \\ &= 0 \end{aligned}$$

in P for every $t \in H^1_{\mathcal{G}}(F,T_P)$. It follows from Poitou-Tate global duality that d is the image of a global class $\delta \in H^1(G_\Sigma, S_{\mathrm{Iw}})$, and that $\tilde{s} - \delta \in H^1_{\mathcal{F}}(F,S_K)$ reduces to $s \in H^1_{\mathcal{F}}(F,S_P)$. This and a similar argument with the roles of S and T reversed show that the kernels on the left and right are contained in the images of

$$H^1_{\mathcal{F}}(F,S_K) \ \to \ H^1_{\mathcal{F}}(F,S_P) \qquad\qquad H^1_{\mathcal{G}}(F,T_K) \ \to \ H^1_{\mathcal{G}}(F,T_P)$$

respectively. The image of $H^1_{\mathcal{F}}(F,S_K)$ is clearly contained in the universal norms which are clearly contained in the left kernel, and similarly for T, and so the kernels on either sides are exactly the universal norms.

The final claim regarding the case $S = T$ follows from the two descriptions of the pairing in (2) and the skew-symmetry of the cup product. Details can be found in Flach's paper. $\square$

Lemma 1.9. *Let*

$$\mathcal{O}_\infty\{1\} = \varinjlim \mathcal{O}_n\{1\} \cong \varinjlim \Lambda_n\{0\},$$

so that $\mathcal{O}_\infty\{1\}$ *is just* $\mathcal{O}_\infty$ *with* G_Σ *acting trivially. For any* Λ*-module of finite type,* A*, the map* $\mathrm{ev} : \mathcal{O}_\infty\{1\} \to \mathcal{O}$ *induces a canonical isomorphism in* $\mathbf{Mod}_\Sigma(\mathcal{O})$

$$\mathrm{Hom}_\Lambda(A, \mathcal{O}_\infty\{1\}) \cong \mathrm{Hom}_\mathcal{O}(A, \mathcal{O}).$$

Proof. This is a special case of Frobenius reciprocity. The inverse map may be described explicitly as follows: for $\phi \in \mathrm{Hom}_\mathcal{O}(A, \mathcal{O})$ we must have $\phi((\gamma^{p^n}-1)A) = 0$ for $n \gg 0$, by discreteness of $\mathcal{O}$ and continuity of ϕ. Taking n very large we then define $\Phi \in \mathrm{Hom}_\Lambda(A, \mathcal{O}_n\{1\})$ by $\Phi(a)(g) = \phi(\omega_{\mathrm{taut}}(g) \cdot a)$ for $g \in G_\Sigma$. □

Keep the assumptions of Theorem 1.8. Fixing a topological generator γ of Γ, the isomorphisms η_γ of Lemma 1.5 determine Selmer structures, still denoted by $\mathcal{F}$ and $\mathcal{G}$, on S_∞ and T_∞, and these Selmer structures do not depend on the choice of γ. The composition

$$P \cong \mathcal{O}_P\{1\} \xrightarrow{\eta_\gamma} \mathcal{O}_\infty\{1\} \xrightarrow{\mathrm{ev}} \mathcal{O} \tag{3}$$

allows us to construct from the pairing of Theorem 1.8 a pairing

$$h_\gamma : H^1_\mathcal{F}(F, S_\infty) \times H^1_\mathcal{G}(F, T_\infty) \to \mathcal{O}$$

whose kernel (by Lemma 1.9) on either side is exactly the submodule of universal norms.

Lemma 1.10. *The above pairing satisfies*

(a) $h_\gamma(\lambda s, t) = h_\gamma(s, \lambda^\iota t)$
(b) *for* $u \in \mathbf{Z}_p^\times$, $h_{\gamma^u}(s,t) = u^{-1}h_\gamma(s,t)$
(c) *if* $S = T$, $\mathcal{F} = \mathcal{G}$, *and the pairing* $S \times T \to \mathcal{O}(1)$ *is symmetric (resp. alternating) then* h_γ *is alternating (resp. symmetric).*

Proof. Let $\phi_\gamma : P \to \mathcal{O}$ be the composition (3), so that

$$h_\gamma(s,t) = \phi_\gamma([\eta_\gamma^{-1}(s), \eta_\gamma^{-1}(t)]).$$

The first equality is then immediate from the corresponding property of the pairing $[\ ,\ ]$. For the second property, we compute

$$h_{\gamma^u}(s,t) = \phi_{\gamma^u}([\eta_{\gamma^u}^{-1}(s), \eta_{\gamma^u}^{-1}(t)]) = u^{-2}\phi_{\gamma^u}([\eta_\gamma^{-1}(s), \eta_\gamma^{-1}(t)])$$

and so it suffices to check $\phi_{\gamma^u} = u\phi_\gamma$, which is clear from the definition. For the third property we must show that $\phi(\mathfrak{p}^\iota) = -\phi(\mathfrak{p})$ for $\mathfrak{p} \in P$. If we write $\mathfrak{p} = \frac{\lambda}{\gamma^{p^n}-1}$ for some integer $n > 0$ and $\lambda \in \Lambda$, then

$$\left(\frac{\lambda}{\gamma^{p^n}-1}\right)^\iota = \frac{-\lambda^\iota}{\gamma^{p^n}-1}$$

in P, and so under the isomorphism $P \xrightarrow{\eta_\gamma} \mathcal{O}_\infty\{1\} \cong \varinjlim \Lambda_n$ the action of ι on P becomes minus the natural action of ι on $\varinjlim \Lambda_n$. For $\lambda \in \Lambda_n$, $\mathrm{ev}(\lambda^\iota) = \mathrm{ev}(\lambda)$ and the claim follows. □

Part (b) of the Lemma implies that the pairing of the following theorem is well defined.

Theorem 1.11. *Keep the assumptions of Theorem 1.8 and let $J \subset \Lambda$ be the augmentation ideal. There is a canonical pairing*

$$h : H^1_{\mathcal{F}}(F, S_\infty) \times H^1_{\mathcal{G}}(F, T_\infty) \ \to \ J/J^2$$

defined by $h(s,t) = h_\gamma(s,t)(\gamma - 1)$ where γ is any topological generator of Γ. This pairing satisfies $h(\lambda s, t) = h(s, \lambda^\iota t)$ and the kernels on either side are exactly the universal norms. If $S = T$, $\mathcal{F} = \mathcal{G}$, and the pairing $T \times T \ \to \ \mathcal{O}(1)$ is symmetric (resp. alternating) then h is alternating (resp. symmetric).

Proof. All of the claims follow easily from Lemmas 1.9 and 1.10, and the properties of the pairing of Theorem 1.8. □

Remark 1.12. Keeping the notation of the thoerem, suppose L is a subfield of F with F_∞/L Galois, and assume that the action of G_F on S and T extends to an action of G_L. Then for $\bullet = \mathrm{Iw}$, P, K, or ∞, the action of Λ on $H^1(F, S_\bullet)$ extends to an action of $\Lambda_L = \mathcal{O}[[\mathrm{Gal}(F_\infty/L)]]$. Similarly for every place v of L the action of Λ on the semi-localization

$$\bigoplus_{w|v} H^1(F_w, S_\bullet)$$

extends to an action of Λ_L. If we assume that the local conditions $\mathcal{F}$ and $\mathcal{G}$ are stable under the action of Λ_L, then Λ_L acts on the associated Selmer groups. The action of $\mathrm{Gal}(F/L)$ on Γ determines a character

$$\omega : \mathrm{Gal}(F/L) \ \to \ \mathbf{Z}_p^\times$$

by $\sigma\gamma\sigma^{-1} = \gamma^{\omega(\sigma)}$ for every $\sigma \in \mathrm{Gal}(F_\infty/L)$ and $\gamma \in \Gamma$. Then for $\sigma \in \mathrm{Gal}(F_\infty/L)$ it can be shown that $h(s^\sigma, t^\sigma) = \omega(\sigma) \cdot h(s,t)$.

2. Derived heights and derivatives of L-functions

Throughout this section we work with fixed objects S and T of $\mathbf{Mod}_\Sigma(\mathcal{O})$, and assume that these modules are in Cartier duality. Let $\mathcal{F}$ and $\mathcal{G}$ be Selmer structures on S_K and T_K, respectively, which are everywhere exact orthogonal complements under the pairing of Lemma 1.6, and let

$$h : H^1_{\mathcal{F}}(F, S_\infty) \times H^1_{\mathcal{G}}(F, T_\infty) \ \to \ J/J^2$$

be the height pairing of Theorem 1.11. We abbreviate

$$Y_S = H^1_{\mathcal{F}}(F, S_\infty) \qquad Y_T = H^1_{\mathcal{G}}(F, T_\infty).$$

Let $Y = Y_S$ or Y_T. For any $r \geq 1$ set $\delta_r(Y) = Y[J^r]/Y[J^{r-1}]$. A choice of topological generator $\gamma \in \Gamma$ determines an injection

$$\phi_{r,\gamma} : \delta_r(Y) \ \to \ Y[J]$$

given by $\phi_{r,\gamma}(y) = (\gamma - 1)^{r-1} y$, and we denote its image by $Y^{(r)} \subset Y[J]$. This image is independent of the choice of γ and defines a decreasing filtration

$$\ldots \subset Y^{(3)} \subset Y^{(2)} \subset Y^{(1)} = Y[J].$$

The intersection $\cap Y^{(r)}$ consists of the elements of $Y[J]$ which are universal norms in Y.

Remark 2.1. We define a Selmer structure on S by propagating $\mathcal{F}$ through the natural inclusion $S \to S_\infty$, and again denote this by $\mathcal{F}$. This inclusion induces a surjective map

$$H^1_{\mathcal{F}}(F, S) \to Y_S[J]$$

whose kernel is bounded (by the inflation-restriction sequence) by the order of the group $H^1(F_\infty/F, H^0(F_\infty, S))$. Similar remarks hold for T.

Definition 2.2. We define the r^{th} derived height

$$h^{(r)} : Y_S^{(r)} \times Y_T^{(r)} \to J^r/J^{r+1}$$

by the composition

$$Y_S^{(r)} \times Y_T^{(r)} \xrightarrow{\phi_{r,\gamma}^{-1} \times \mathrm{id}} \delta_r(Y_S) \times Y_T^{(r)} \xrightarrow{h} J/J^2 \xrightarrow{(\gamma-1)^{r-1}} J^r/J^{r+1}.$$

It is easily checked that this is independent of the choice of γ. Note that $h^{(1)}$ is nothing more than the restriction of h to $Y_S[J] \times Y_T[J]$.

If $S = T$ and $\mathcal{F} = \mathcal{G}$, then for any $x, y \in Y_S$,

$$h^{(r)}(x, y) = \begin{cases} (-1)^r h^{(r)}(y, x) & \text{if } e \text{ symmetric} \\ (-1)^{r+1} h^{(r)}(y, x)) & \text{if } e \text{ alternating.} \end{cases}$$

The following lemma implies that the kernels of $h^{(r)}$ on the left and right are $Y_S^{(r+1)}$ and $Y_T^{(r+1)}$, respectively.

Lemma 2.3. *If $\lambda_0, \lambda_1 \in \Lambda$ are distinguished then the kernels on the left and right of the restriction of h to $Y_S[\lambda_0] \times Y_T[\lambda_1]$ are the images of*

$$Y_S[\lambda_0 \lambda_1^\iota] \xrightarrow{\lambda_1^\iota} Y_S[\lambda_0] \qquad Y_T[\lambda_0^\iota \lambda_1] \xrightarrow{\lambda_0^\iota} Y_T[\lambda_1]$$

respectively.

Proof. Let Z_S and Z_T be the quotients of Y_S and Y_T by the submodules of universal norms. The natural map

$$Y_S[\lambda_0]/\lambda_1^\iota Y_S[\lambda_1^\iota \lambda_0] \to Z_S[\lambda_0]/\lambda_1^\iota Z_S[\lambda_1^\iota \lambda_0] \to Z_S/\lambda_1^\iota Z_S$$

is an injection, and the height pairing defines an injection

$$Z_S/\lambda_1^\iota Z_S \cong \mathrm{Hom}(Z_T[\lambda_1], J/J^2) \to \mathrm{Hom}(Y_T[\lambda_1], J/J^2).$$

This shows that

$$Y_S[\lambda_0 \lambda_1^\iota] \xrightarrow{\lambda_1^\iota} Y_S[\lambda_0] \to \mathrm{Hom}(Y_T[\lambda_1], J/J^2)$$

is exact. The kernel on the right is computed similarly. □

The pairing e_{Iw} of Lemma 1.6 induces a perfect pairing

$$e_P : S_{\mathrm{Iw}} \times T_P \to P(1).$$

The identification $T_P \cong T_\infty$ of Lemma 1.5 and the map (3), both of which depend on a choice of topological generator, induce a perfect pairing

$$e_\infty : S_{\mathrm{Iw}} \times T_\infty \to \mathcal{O}(1)$$

which does not depend on the choice of generator. If one views S_{Iw} as the space of S-valued measures on Γ, and T_∞ as the spaces of locally constant T-valued functions on Γ, then this pairing is integration. Using Lemma 1.9, it can be checked

that the local conditions $\mathcal{F}$ and $\mathcal{G}$ on S_{Iw} and T_∞ are everwhere exact orthogonal complements under the local Tate pairing

$$H^1(F_v, S_{\mathrm{Iw}}) \times H^1(F_v, T_\infty) \ \to \ \mathcal{O}$$

induced by e_∞.

Denote by $\mathcal{F}^{\mathrm{rel}}$ the Selmer structure on S_{Iw} whose local conditions at places of F not dividing p are the same as those of $\mathcal{F}$, but with no condition imposed at primes above p. At any place v of F we denote

$$H^1_{/\mathcal{F}}(F_v, S_{\mathrm{Iw}}) = H^1(F_v, S_{\mathrm{Iw}})/H^1_{\mathcal{F}}(F_v, S_{\mathrm{Iw}}),$$

and we let

$$H^1_\bullet(F_p, \ \ ) = \bigoplus_{v|p} H^1_\bullet(F_v, \ \ )$$

denote the semi-local cohomology at p, where $\bullet$ is either $\mathcal{F}$ or $/\mathcal{F}$. Using the fact that the local condition $\mathcal{F}$ on S_{Iw} is propagated from a local condition on S_K, it is easy to see that $H^1_{/\mathcal{F}}(F_v, S_{\mathrm{Iw}})[f] = 0$ for any place v of F and any distinguished $f \in \Lambda$.

For the motivation behind the following definition, see [13], [14], or [15].

Definition 2.4. For any element

$$z = \{z_n\} \in \varprojlim H^1_{\mathcal{F}^{\mathrm{rel}}}(F, S_n) \cong H^1_{\mathcal{F}^{\mathrm{rel}}}(F, S_{\mathrm{Iw}})$$

define the p-adic L-function of z, $\mathcal{L}_z$, to be the image of z in

$$H^1_{/\mathcal{F}}(F_p, S_{\mathrm{Iw}}) \cong \mathrm{Hom}(H^1_{\mathcal{G}}(F_p, T_\infty), \mathcal{O}).$$

Define the order of vanishing of $\mathcal{L}_z$, $\mathrm{ord}(\mathcal{L}_z)$, to be the largest power of J by which $\mathcal{L}_z$ is divisible in $H^1_{/\mathcal{F}}(F_p, S_{\mathrm{Iw}})$. Equivalently, $\mathrm{ord}(\mathcal{L}_z)$ is the largest integer r such that

$$\mathcal{L}_z(H^1_{\mathcal{G}}(F_p, T_\infty)[J^r]) = 0.$$

For any topological generator $\gamma \in \Gamma$ and any $r \leq \mathrm{ord}(\mathcal{L}_z)$ we define $\mathrm{Der}^r_\gamma(\mathcal{L}_z)$ to be the preimage of $\mathcal{L}_z$ under the injection

$$H^1_{/\mathcal{F}}(F_p, S_{\mathrm{Iw}}) \ \xrightarrow{(\gamma-1)^r} \ H^1_{/\mathcal{F}}(F_p, S_{\mathrm{Iw}}).$$

Define

$$\mathcal{L}_z^{(r)} : H^1_{\mathcal{G}}(F_p, T_\infty) \ \to \ J^r/J^{r+1}$$

by $\mathcal{L}_z^{(r)}(c) = \mathrm{Der}^r_\gamma(\mathcal{L}_z)(c) \cdot (\gamma - 1)^r$. Then $\mathcal{L}_z^{(r)}$ is independent of the choice of γ. The restriction of $\mathcal{L}_z^{(r)}$ to $H^1_{\mathcal{G}}(F_p, T_\infty)[J]$ should be thought of as the "special value" of the r^{th} derivative of $\mathcal{L}_z$, and we denote it by $\lambda_z^{(r)}$.

The following is a higher derivative version of Theorem 1 of [14]. Note that the theorem asserts that a local divisibility (of the p-adic L-function $\mathcal{L}_z$ by a power of J) implies a global divisibility (of z_0 by a power of J).

Theorem 2.5. *Keep notation as above, with $r \leq \mathrm{ord}(\mathcal{L}_z)$, and propagate the Selmer structure $\mathcal{F}$ to S via $S_{\mathrm{Iw}} \ \to \ S$. This is equal to the Selmer structure obtained by propagation through $S \ \to \ S_\infty$. Then*

(a) $\lambda_z^{(0)} = 0$ *if and only if* $z_0 \in H^1_{\mathcal{F}}(F, S)$,
(b) $\lambda_z^{(r)} = 0$ *if and only if* $r < \mathrm{ord}(\mathcal{L}_z)$,

(c) *suppose* $0 < r \leq \mathrm{ord}(\mathcal{L}_z)$, *then* $z_0 \in Y_S^{(r)}$ *and for any* $c \in Y_T^{(r)}$

$$h^{(r)}(z_0, c) = \lambda_z^{(r)}(c_p),$$

where c_p *is the image of* c *in* $H^1_{\mathcal{G}}(F_p, T_\infty)$.

Proof. Fix a topological generator $\gamma \in \Gamma$. We have $\lambda_z^{(0)} = 0$ if and only if $\mathcal{L}_z$ is divisible by J. The first claim now follows from exactness of

$$H^1_{/\mathcal{F}}(F_p, S_{\mathrm{Iw}}) \xrightarrow{\gamma-1} H^1_{/\mathcal{F}}(F_p, S_{\mathrm{Iw}}) \to H^1_{/\mathcal{F}}(F_p, S).$$

For the second, $r < \mathrm{ord}(\mathcal{L}_z)$ if and only if $\mathrm{Der}^r_\gamma(\mathcal{L}_z)$ is divisible by $\gamma - 1$ in $H^1_{/\mathcal{F}}(F_p, S_{\mathrm{Iw}})$, and this is equivalent, by local duality, to $\mathrm{Der}^r_\gamma(\mathcal{L}_z)$ vanishing on the J-torsion in $H^1_{\mathcal{G}}(F, T_\infty)$.

For the third claim, first suppose $z_0 \in Y_S^{(r)}$ and fix $c \in Y_T^{(r)}$. Let $\tilde{z} \in H^1_{\mathcal{F}^{\mathrm{rel}}}(F, S_K)$ be defined by $\tilde{z} = z \otimes (\gamma - 1)^{-r}$ and let y denote the image of $\tilde{z}$ in $H^1_{\mathcal{F}^{\mathrm{rel}}}(F, S_P)$. Under the map

$$H^1(F, S_P) \xrightarrow{\eta_\gamma} H^1(F, S_\infty)$$

of Lemma 1.5, $(\gamma - 1)^{r-1} y$ maps to z_0. Since we are assuming that $z_0 \in Y_S^{(r)}$ and $c \in Y_T^{(r)}$, we may choose $s \in H^1_{\mathcal{F}}(F, S_P)$ and $d \in H^1_{\mathcal{G}}(F, T_P)$ which satisfy

$$(\gamma - 1)^{r-1} \eta_\gamma(s) = z_0 \qquad (\gamma^{-1} - 1)^{r-1} \eta_\gamma(d) = c.$$

We have $(\gamma - 1)^{r-1} \eta_\gamma(s - y) = 0$, and so

$$\begin{aligned} h^{(r)}(z_0, c) &= (\gamma - 1)^{r-1} \cdot h(\eta_\gamma(s), c) \\ &= (\gamma - 1)^{r-1} \cdot h(\eta_\gamma(y), c). \end{aligned}$$

Unraveling the definition of h, we find

$$h(\eta_\gamma(y), c) = (\gamma - 1) \cdot \phi_\gamma\big([y, (\gamma^{-1} - 1)^{r-1} d]\big)$$

where ϕ_γ is the composition (3) and [,] is the pairing of Theorem 1.8. Choose a lift, $\tilde{d}_p$, of $\mathrm{loc}_p(d)$ to $H^1_{\mathcal{G}}(F_p, T_K)$, and let $\tilde{c}_p = (\gamma^{-1} - 1)^{r-1} \tilde{d}_p$. We now have

$$\begin{aligned} \phi_\gamma\big([y, (\gamma^{-1} - 1)^{r-1} d]\big) &= \phi_\gamma\big(\mathrm{inv}_p\big((\gamma - 1)^{r-1} y \cup \tilde{d}_p\big)\big) \\ &= \phi_\gamma\big(\mathrm{inv}_p\big(\tilde{z} \cup (\gamma^{-1} - 1)^{-r} \tilde{c}_p\big)\big) \\ &= \mathrm{Der}^r_\gamma(\mathcal{L}_z)(c_p). \end{aligned}$$

Combining all of this gives

$$h^{(r)}(z_0, c) = (\gamma - 1)^r \cdot \mathrm{Der}^r_\gamma(\mathcal{L}_z)(c_p) = \lambda_z^{(r)}(c_p).$$

We now show by induction on r that $z_0 \in Y_S^{(r)}$ for $1 \leq r \leq \mathrm{ord}(\mathcal{L}_z)$. The case $r = 1$ follows from parts (a) and (b): since $0 < \mathrm{ord}(\mathcal{L}_z)$ we must have $z_0 \in H^1_{\mathcal{F}}(F, S_\infty)[J]$. For the inductive step, if $z_0 \in Y_S^{(r-1)}$ then we have shown that

$$h^{(r-1)}(z_0, c) = \lambda_z^{(r-1)}(c_p)$$

for every $c \in Y_T^{(r-1)}$. But since $r - 1 < \mathrm{ord}(\mathcal{L}_z)$, part (b) of the proposition implies that $\lambda_z^{(r-1)}(c_p) = 0$ and we conclude that z_0 is in the kernel on the left of $h^{(r-1)}$. This kernel is exactly $Y_S^{(r)}$, and the claim is proven. □

3. Selmer groups of ordinary abelian varieties

Let A be an abelian variety defined over F and let $A^\vee$ be the dual abelian variety. We assume throughout that A has good ordinary reduction at all primes of F above p, and that the primes of bad reduction are finitely decomposed in F_∞. Assume further that p does not ramify in F, but that all primes of F above p do ramify in F_∞. We wish to prove the following: for each power p^k of p there are generalized Selmer groups

$$H^1_{\mathcal{F}}(F_\infty, A[p^k]) \subset H^1(F_\infty, A[p^k]) \qquad H^1_{\mathcal{F}^\vee}(F_\infty, A^\vee[p^k]) \subset H^1(F_\infty, A^\vee[p^k])$$

such that the inclusion $A[p^k] \hookrightarrow A[p^\infty]$ induces a map of Λ-modules

$$H^1_{\mathcal{F}}(F_\infty, A[p^k]) \ \to\ \mathrm{Sel}_{p^\infty}(A/F_\infty)[p^k]$$

whose kernel and cokernel are finite and bounded as k varies (and similarly for $A^\vee$), where $\mathrm{Sel}_{p^\infty}(A/F_\infty)$ is the usual p-power Selmer group associated to A. These generalized Selmer groups are of the type described in Section 1, and so there is a height pairing

$$h_k : H^1_{\mathcal{F}}(F_\infty, A[p^k]) \times H^1_{\mathcal{F}^\vee}(F_\infty, A^\vee[p^k]) \ \to\ J_k/J_k^2$$

where J_k denotes the augmentation ideal of $(\mathbf{Z}/p^k\mathbf{Z})[[\Gamma]]$, and this pairing enjoys all the properties of that of Theorem 1.11.

For every place of F, fix once and for all an extension to $\bar{F}$. At any place v of F above p and for any k we let $\mathrm{Fil}_v A[p^k]$ be the kernel of the reduction map

$$A(\bar{F}_v)[p^k] \ \to\ \tilde{A}[p^k]$$

where $\tilde{A}$ is the reduction of A at v. Define $\mathrm{Fil}_v A^\vee[p^k]$ similarly. Define $\mathrm{gr}_v A[p^k]$ by exactness of

$$0 \ \to\ \mathrm{Fil}_v A[p^k] \ \to\ A(\bar{F}_v)[p^k] \ \to\ \mathrm{gr}_v A[p^k] \ \to\ 0 \tag{4}$$

and similarly for $A^\vee$. The reduction map on p^k-torsion is surjective, and so $\mathrm{gr}_v A[p^k] \cong \tilde{A}[p^k]$.

Lemma 3.1. *The submodules* $\mathrm{Fil}_v A[p^k]$ *and* $\mathrm{Fil}_v A^\vee[p^k]$ *are exact orthogonal complements under the Weil pairing.*

Proof. The assumption that A has ordinary reduction ensures that $\mathrm{Fil}_v A[p^k]$ and $\mathrm{Fil}_v A^\vee[p^k]$ have exact order p^{kg}, where $g = \dim(A)$. As modules for the inertia group $\mathcal{I}_v$ of v, each is isomorphic to a product of copies of μ_{p^k}, and there are nonontrivial $\mathcal{I}_v$ invariant pairings $\mu_{p^k}^g \times \mu_{p^k}^g \ \to\ \mu_{p^k}$. □

We set $\mathcal{O} = \mathbf{Z}/p^k\mathbf{Z}$, $S = A[p^k]$, and $T = A^\vee[p^k]$ and use the notation of the first section. Shapiro's lemma and Lemma 1.5 allow us to identify

$$H^1(F_\infty, A[p^k]) \cong H^1(F, S_\infty) \cong H^1(F, S_P). \tag{5}$$

For $\bullet = \mathrm{Iw}$, K, P, or ∞, and any place v of F above p, the submodule $\mathrm{Fil}_v S \subset S$ induces a submodule $\mathrm{Fil}_v S_\bullet \subset S_\bullet$ in an obvious way, and similarly with S replaced by T or with Fil_v replaced by gr_v.

Following Coates and Greenberg [4], we make the

Definition 3.2. We define a Selmer structure, $\mathcal{F}$, on S_K by setting

$$H^1_{\mathcal{F}}(F_v, S_K) = \begin{cases} H^1_{\mathrm{unr}}(F_v, S_K) & \text{if } v \nmid p \\ \mathrm{image}\big(H^1(F_v, \mathrm{Fil}_v S_K) \ \to\ H^1(F_v, S_K)\big) & \text{if } v \mid p \end{cases}$$

and define $\mathcal{F}^\vee$ on T_K similarly.

The local conditions $\mathcal{F}$ and $\mathcal{F}^\vee$ are everywhere exact orthogonal complements under the local Tate pairing induced by the Weil pairing and Lemma 1.6. We use the Selmer group $H^1_{\mathcal{F}}(F, S_P)$ and the identification (5) to define a Selmer group $H^1_{\mathcal{F}}(F_\infty, A[p^k])$, and make the definition for $A^\vee$ similarly.

We must compare these generalized Selmer groups with the usual definitions. Let

$$\mathrm{Fil}_v\mathbf{S} = \varinjlim(\mathrm{Fil}_v S_\infty) \qquad \mathbf{S} = \varinjlim S_\infty$$

where the limits are over k. Shapiro's lemma identifies $H^1(F, \mathbf{S}) \cong H^1(F_\infty, A[p^\infty])$ and for any place v of F

$$H^1(F_v, \mathbf{S}) \cong \varinjlim \bigoplus_w H^1(F_{n,w}, A[p^\infty])$$

where the sum is over places w of F_n lying above v.

Definition 3.3. Define the ordinary Selmer structure on $\mathbf{S}[p^k]$ by

$$H^1_{\mathrm{ord}}(F_v, \mathbf{S}[p^k]) = \begin{cases} H^1_{\mathrm{unr}}(F_v, \mathbf{S}[p^k]) & \text{else} \\ \mathrm{image}\big(H^1(F_v, \mathrm{Fil}_v\mathbf{S}[p^k]) \ \to \ H^1(F_v, \mathbf{S}[p^k])\big) & \text{if } v \mid p \end{cases}$$

and let $H^1_{\mathrm{ord}}(F, \mathbf{S}) = \varinjlim H^1_{\mathrm{ord}}(F, \mathbf{S}[p^k])$.

Proposition 3.4. *The isomorphism $H^1(F, \mathbf{S}) \cong H^1(F_\infty, A[p^\infty])$ identifies*

$$H^1_{\mathrm{ord}}(F, \mathbf{S}) \cong \mathrm{Sel}_{p^\infty}(A/F_\infty).$$

Proof. Let Σ be the set of primes of F containing all archimedean primes, primes above p, and primes at which A has bad reduction, and let F_Σ be the maximal extension of F unramified outside Σ. Then both Selmer groups are defined as the subgroup of $H^1(F_\Sigma/F_\infty, A[p^\infty])$ of elements which are locally trivial at every $v \in \Sigma$ not dividing p (this follows from Lemma 1.7 and Proposition 1.6.8 of [16]), and are in the kernel of reduction

$$H^1(F_{\infty,w}, A[p^\infty]) \ \to \ H^1(F_{\infty,w}, \tilde{A}[p^\infty])$$

at places above p. This description of the image of the Kummer map for $w \mid p$ can be found in [4], in particular Proposition 4.3. □

Proposition 3.5. *There are natural maps*

$$H^1_{\mathcal{F}}(F_\infty, A[p^k]) \ \to \ H^1_{\mathrm{ord}}(F, \mathbf{S}[p^k]) \ \to \ H^1_{\mathrm{ord}}(F, \mathbf{S})[p^k]$$

whose kernels and cokernels are finite and bounded as k varies.

Proof. For the first arrow, let $S = A[p^k]$, $\mathcal{O} = \mathbf{Z}/p^k\mathbf{Z}$, and recall the identifications $\mathbf{S}[p^k] \cong S_\infty \cong S_P$. The first arrow becomes the inclusion

$$H^1_{\mathcal{F}}(F, S_P) \subset H^1_{\mathrm{ord}}(F, S_P). \tag{6}$$

The local conditions defining both Selmer groups are unramified (using Lemma 1.7 for $\mathcal{F}$) away from p. Above p, the local condition $H^1_{\mathcal{F}}(F_v, S_P)$ is defined as the image of the composition

$$H^1(F_v, \mathrm{Fil}_v S_K) \ \to \ H^1(F_v, \mathrm{Fil}_v S_P) \ \to \ H^1(F_v, S_P),$$

while the ordinary local condition is defined as the image of the second arrow. It follows that we have injections

$$\begin{aligned} H^1_{\mathrm{ord}}(F,S_P)/H^1_{\mathcal{F}}(F,S_P) &\to \bigoplus_v H^1(F_v,\mathrm{Fil}_v S_P)/H^1(F_v,\mathrm{Fil}_v S_K) \\ &\to \bigoplus_v H^2(F_v,\mathrm{Fil}_v S_{\mathrm{Iw}}) \end{aligned}$$

where the sums are over the primes v of F above p. By local duality and Shapiro's lemma the order of $H^2(F_v,\mathrm{Fil}_v S_{\mathrm{Iw}})$ is bounded by

$$\bigoplus_v H^0(F_v,\mathrm{gr}_v T_\infty) \cong \bigoplus_{w|p} \tilde{A}^\vee(L_w)[p^k]$$

where $T=A^\vee[p^k]$, the second sum is over all primes of F_∞ above p, L_w denotes the residue field of F_∞ at w, and $\tilde{A}^\vee$ is the reduction of $A^\vee$ at w. This group is finite and bounded as k varies, by the assumption that all primes of F above p ramify in F_∞.

To control the kernel and cokernel of

$$H^1_{\mathrm{ord}}(F,\mathbf{S}[p^k]) \to H^1_{\mathrm{ord}}(F,\mathbf{S})[p^k] \tag{7}$$

we use the exact sequence

$$0 \to A(F_\infty)[p^\infty]/p^k A(F_\infty)[p^\infty] \to H^1(F,\mathbf{S}[p^k]) \to H^1(F,\mathbf{S})[p^k] \to 0$$

The kernel of (7) is bounded by the order of $A(F_\infty)[p^\infty]$ modulo its maximal divisible subgroup. By the snake lemma, to bound the cokernel of (7) it suffices to bound the kernel of

$$\bigoplus_v H^1(F_v,\mathbf{S}[p^k])/H^1_{\mathrm{ord}}(F_v,\mathbf{S}[p^k]) \to \bigoplus_v H^1(F_v,\mathbf{S})/H^1_{\mathrm{ord}}(F_v,\mathbf{S})$$

and we compute this kernel term by term in three cases.

Suppose first that v does not divide p, and that A has good reduction at v. Then the kernel of

$$H^1(F_v,\mathbf{S}[p^k])/H^1_{\mathrm{ord}}(F_v,\mathbf{S}[p^k]) \to H^1(F_v,\mathbf{S})/H^1_{\mathrm{ord}}(F_v,\mathbf{S}) \tag{8}$$

injects into the kernel of $H^1(F_v^{\mathrm{unr}},\mathbf{S}[p^k]) \to H^1(F_v^{\mathrm{unr}},\mathbf{S})$ which is

$$H^0(F_v^{\mathrm{unr}},\mathbf{S})/p^k H^0(F_v^{\mathrm{unr}},\mathbf{S}) \cong \mathbf{S}/p^k\mathbf{S} = 0.$$

If v does not divide p and A has bad reduction at v, then our assumption that v is finitely decomposed in F_∞ implies that

$$H^1_{\mathrm{ord}}(F_v,\mathbf{S}) = H^1_{\mathrm{ord}}(F_v,\mathbf{S}[p^k]) = 0$$

by Lemma 1.7, and so we must bound the kernel of the map

$$H^1(F_v,\mathbf{S}[p^k]) \to H^1(F_v,\mathbf{S}).$$

This kernel is $H^0(F_v,\mathbf{S})/p^k H^0(F_v,\mathbf{S})$ which has order bounded by the size of the quotient of $\bigoplus A(F_{\infty,w})[p^\infty]$ by its maximal divisible subgroup, where the sum is over primes w of F_∞ above v.

Lastly, if $v \mid p$ it suffices to bound the kernel of

$$H^1(F_v,\mathrm{gr}_v\mathbf{S}[p^k]) \to H^1(F_v,\mathrm{gr}_v\mathbf{S}).$$

This kernel is controlled by the order of

$$H^0(F_v, \mathrm{gr}_v \mathbf{S}) \cong \bigoplus_w \tilde{A}(L_w)[p^\infty]$$

modulo its maximal divisible subgroup, where the sum is over primes of F_∞ above p, L_w is the residue field F_∞ at w, and $\tilde{A}$ is the reduction of A at v. □

4. Semi-simplicity of Iwasawa modules

We now set $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$, let J be the augmentation ideal of Λ, and denote by $I_n \subset \Lambda$ the kernel of the natural projection $\Lambda \to \mathbf{Z}_p[\mathrm{Gal}(F_n/F)]$, so that $I_0 = J$. Keep $A_{/F}$ as in the preceeding section, so that A has good ordinary reduction at all primes of F above p, the primes of bad reduction are finitely decomposed in F_∞, p does not ramify in F, and all primes of F above p do ramify in F_∞.

Let $Y_k = H^1_{\mathcal{F}}(F_\infty, A[p^k])$ be the generalized Selmer group of Section 3, and set $Y_k(F_n) = Y_k[I_n]$. We denote by

$$\ldots \subset Y_k^{(3)} \subset Y_k^{(2)} \subset Y_k^{(1)} = Y_k(F)$$

the filtration of Section 2. The surjection $A[p^{k+1}] \xrightarrow{p} A[p^k]$ induces a map $Y_{k+1}^{(r)} \to Y_k^{(r)}$, and we define

$$Y_\infty^{(r)} = \varprojlim Y_k^{(r)} \qquad Y_\infty(F_n) = \varprojlim Y_k(F_n)$$

so that $Y_\infty^{(r)}$ defines a decreasing filtration of $Y_\infty(F)$. Set

$$Y = \mathrm{Sel}_{p^\infty}(A/F_\infty) \qquad X = \mathrm{Hom}_{\mathbf{Z}_p}(Y, \mathbf{Q}_p/\mathbf{Z}_p).$$

These are cofinitely and finitely generated Λ-modules, respectively. By Propositions 3.4 and 3.5 we have canonical maps $Y_k \to Y[p^k]$ with kernel and cokernel finite and bounded as k varies, and these induce maps

$$Y_k^{(r)} \cong Y_k[J^r]/Y_k[J^{r-1}] \to (Y[J^r]/Y[J^{r-1}])[p^k]$$

whose kernels and cokernels are again finite and bounded as k varies. The $\mathbf{Z}_p$-module $Y[J^r]/Y[J^{r-1}]$ is cofinitely generated, and so

$$\begin{aligned} \mathrm{rank}(Y_\infty^{(r)}) &= \mathrm{rank}\left(\varprojlim (Y[J^r]/Y[J^{r-1}])[p^k]\right) \\ &= \mathrm{corank}(Y[J^r]/Y[J^{r-1}]) \\ &= \mathrm{rank}(J^{r-1}X/J^rX). \end{aligned} \tag{9}$$

Lemma 4.1. *Define* $S_p(A/F_n) = \varprojlim \mathrm{Sel}_{p^k}(A/F_n)$. *There is a canonical isomorphism*

$$Y_\infty(F_n) \otimes \mathbf{Q}_p \xrightarrow{j} S_p(A/F_n) \otimes \mathbf{Q}_p.$$

Furthermore this isomorphism is semi-integral *in the sense that there are integers* t_0, t_1, *independent of* n, *such that* $p^{t_0} j(Y_\infty(F_n))$ *is contained the lattice generated by* $S_p(A/F_n)$, *and* $p^{t_1} j^{-1}(S_p(A/F_n))$ *is contained in the lattice generated by* $Y_\infty(F_n)$.

Proof. We have maps

$$Y_k(F_n) \to \mathrm{Sel}_{p^\infty}(A/F_\infty)[I_n + p^k\Lambda] \leftarrow \mathrm{Sel}_{p^\infty}(A/F_n)[p^k]$$

whose kernels and cokernels are finite and bounded as both k and n vary (the second arrow by Mazur's control theorem [8]), and so taking the inverse limit in k and tensoring with $\mathbf{Q}_p$ we obtain a semi-integral isomorphism

$$Y_\infty(F_n) \otimes \mathbf{Q}_p \cong (\varprojlim \mathrm{Sel}_{p^\infty}(A/F_n)[p^k]) \otimes \mathbf{Q}_p. \tag{10}$$

For every k there is a canonical surjection

$$\mathrm{Sel}_{p^k}(A/F_n) \ \to \ \mathrm{Sel}_{p^\infty}(A/F_n)[p^k] \tag{11}$$

and these maps are compatible, in the obvious sense, as k varies. As k varies the kernels are uniformly bounded by the order of the finite group $A(F_n)[p^\infty]$, and so passing to the inverse limit over k and tensoring with $\mathbf{Q}_p$, we see that the right hand side of (10) is isomorphic to $S_p(A/F_n) \otimes \mathbf{Q}_p$. Surjectivity of (11) implies that this isomorphism identifies the lattices generated by $\varprojlim \mathrm{Sel}_{p^\infty}(A/F_n)[p^k]$ and $S_p(A/F_n)$. □

The subspace of $S_p(A/F) \otimes \mathbf{Q}_p$ generated by the image of $Y_\infty^{(r)}$ under the isomorphism

$$Y_\infty(F) \otimes \mathbf{Q}_p \ \to \ S_p(A/F) \otimes \mathbf{Q}_p \tag{12}$$

will be denoted $S_p^{(r)}(A/F)$, and we set $S_p^{(\infty)}(A/F) = \cap_r S_p^{(r)}(A/F)$. Let W_r be the one-dimensional $\mathbf{Q}_p$-vector space

$$W_r = (J^r/J^{r+1}) \otimes \mathbf{Q}_p.$$

The derived height pairings of Section 2 are compatible as k varies, and passage to the limit yields the pairing of the following theorem.

Theorem 4.2. *There is a filtration*

$$\ldots \subset S_p^{(3)}(A/F) \subset S_p^{(2)}(A/F) \subset S_p^{(1)}(A/F) = S_p(A/F) \otimes \mathbf{Q}_p$$

such that $\dim_{\mathbf{Q}_p} S_p^{(r)}(A/F) = \mathrm{rank}(J^{r-1}X/J^rX)$ *(and similarly for* $A^\vee$*), and a sequence of pairings*

$$h^{(r)} : S_p^{(r)}(A/F) \times S_p^{(r)}(A^\vee/F) \ \to \ W_r$$

such that the kernel on the left (resp. right) is $S_p^{(r+1)}(A/F)$ *(resp.* $S_p^{(r+1)}(A^\vee/F)$*).*

The subspace $S_p^{(\infty)}(A/F)$ *is the subspace of* universal norms *in the usual sense. That is,* $S_p^{(\infty)}(A/F)$ *is the subspace generated by the intersection over* n *of the image of corestriction* $S_p(A/F_n) \ \to \ S_p(A/F)$*. Furthermore, if* $\phi : A \ \to \ A^\vee$ *is a polarization then* $h^{(r)}$ *satisfies*

$$h^{(r)}(a, \phi(b)) = (-1)^{r+1} h^{(r)}(b, \phi(a))$$

for all $a, b \in S_p^{(r)}(A/F)$*.*

Proof. All of the claims are immediate from the corresponding properties of the derived heights over discrete coefficient rings, together with the equality (9), except for the characterization of $S_p^{(\infty)}(A/F)$. Suppose $x \in S_p^{(\infty)}(A/F)$. Then for some integer t there is a $y \in Y_\infty(F)$, contained in $Y_\infty^{(r)}$ for every r, such that y maps to $p^t x$ under (12). Fix a topological generator $\gamma \in \Gamma$ and set $g_n = \frac{\gamma^{p^n}-1}{\gamma-1} \in \Lambda$. If y_k denotes the image of y in $Y_k(F)$, we claim that y_k is in the image of $g_n : Y_k(F_n) \ \to \ Y_k(F)$ for every n. Indeed, $y_k \in (\gamma-1)^r Y_k$ for every r, and it follows from Lemma 1.2

that y_k is a universal norm (in the sense of Definition 1.3) in Y_k. In particular y_k is divisible by every g_n. Passing to the limit, we must have that y is in the image of $g_n : Y_\infty(F_n) \to Y_\infty(F)$ for every n, say $y = g_n z_n$. If t_0 is as in Lemma 4.1, then the image of $p^{t_0} z_n$ in $S_p(A/F_n) \otimes \mathbf{Q}_p$ is integral and corestricts to $p^{t+t_0}x$. Hence $p^{t+t_0}x$ is a universal norm. The opposite implication is entirely similar. □

By the structure theorem for finitely-generated Iwasawa modules, we may fix a pseudo-isomorphism of Λ-modules

$$X \sim \Lambda^{e_\infty} \oplus M \oplus M'$$

such that M' is a torsion Λ-module with characteristic ideal prime to J, and M has the form

$$M \cong (\Lambda/J)^{e_1} \oplus (\Lambda/J^2)^{e_2} \oplus \dots.$$

The first statement of the following is due to Perrin-Riou [12].

Corollary 4.3. *The integers e_i satisfy the following properties:*

(a) *the height pairing $h^{(1)}$ is nondegenerate if and only if $e_i = 0$ for $1 < i \leq \infty$,*
(b) $e_\infty = \dim_{\mathbf{Q}_p} S_p^{(\infty)}(A/F)$,
(c) $e_r = \dim_{\mathbf{Q}_p} \left(S_p^{(r)}(A/F)/S_p^{(r+1)}(A/F)\right)$,
(d) $e_r \equiv 0 \pmod 2$ *when r is even.*

Proof. By Theorem 4.2 we have the equality

$$\dim_{\mathbf{Q}_p} S_p^{(r)}(A/F) = \operatorname{rank}_{\mathbf{Z}_p}(J^{r-1}X/J^rX) = e_r + e_{r+1} + e_{r+2} + \dots + e_\infty$$

which proves all but the final claim. A choice of polarization of A determines an isomorphism

$$S_p^{(r)}(A/F) \cong S_p^{(r)}(A^\vee/F)$$

and the induced height pairing on $S_p^{(r)}(A/F)$ is alternating when r is even, by the last part of Theorem 4.2. This implies that $S_p^{(r)}(A/F)/S_p^{(r+1)}(A/F)$ is even dimensional. □

In the case where F_∞ is the cylotomic $\mathbf{Z}_p$-extension, it is conjectured that $h^{(1)}$ is nondegenerate. When $F = \mathbf{Q}$ and A is modular it is known by the work of Kato that $e_\infty = 0$ (i.e. X is a torsion module), but it is not known that $e_i = 0$ for $i > 1$.

Now suppose that F is a quadratic imaginary field, F_∞ is the anticyclotomic $\mathbf{Z}_p$-extension, and $A = E \times_{\mathbf{Q}} F$ for some elliptic curve $E_{/\mathbf{Q}}$ satisfying the "Heegner hypothesis" that all primes of bad reduction are split in F (which, in particular, implies our hypothesis that the primes of bad reduction of A are finitely decomposed in F_∞). In this situation it is known by the work of Bertolini [2] and Cornut [5] that $e_\infty = 1$, hence $h^{(r)}$ is degenerate for every r. The next best thing one could hope for is that $S_p^{(2)}(A/F)$ is one dimensional, hence equal to $S_p^{(\infty)}(A/F)$, but this is still too optimistic. By Remark 1.12, $h^{(1)}$ satisfies

$$h^{(1)}(x^\tau, y^\tau) = -h^{(1)}(x, y),$$

where τ is complex conjugation. This forces the plus and minus eigencomponents of $S_p^{(1)}(A/F)$ under τ to be self-orthogonal, and so if

$$s^+ = \dim_{\mathbf{Q}_p} S_p^{(1)}(A/F)^+ \qquad s^- = \dim_{\mathbf{Q}_p} S_p^{(1)}(A/F)^-,$$

the kernel of $h^{(1)}$ has dimension at least $|s^+ - s^-|$.

Conjecture 4.4. *(Bertolini-Darmon, Mazur) In the situation above, the dimension of $S_p^{(2)}(A/F)$ is $|s^+ - s^-|$, and the dimension of $S_p^{(3)}(A/F)$ is 1.*

Assuming the conjecture, Corollary 4.3 implies that $e_2 = |s^+ - s^-| - 1$. Mazur's control theorem gives

$$s^+ + s^- = \dim_{\mathbf{Q}_p} S_p^{(1)}(A/F) = 1 + e_1 + e_2$$

and so

$$X \sim \Lambda \oplus (\Lambda/J)^{e_1} \oplus (\Lambda/J^2)^{e_2} \oplus M'$$

with $e_1 = 2\min\{s^+, s^-\}$ and M' having characteristic ideal prime to J.

Returning to the general case, we wish to reformulate Theorem 2.5 in the present setting. This is merely an exercise in passing from results on $A[p^k]$ to results on the Tate module $T_p(A)$, although some caution is needed, owing to our slightly strange choice of Selmer structures on $A[p^k]$. Let Σ be the set of places of F consisting of all archimedean places and all primes at which A has bad reduction. Define

$$\begin{aligned} H^1_{\mathrm{Iw}}(F_\Sigma/F_\infty, T_p(A)) &= \varprojlim H^1(F_\Sigma/F_n, T_p(A)) \\ Z_\infty &= \varprojlim \oplus_{v|p} H^1(F_{n,v}, T_p(A)) \\ Z_{\infty,f} &= \varprojlim \oplus_{v|p} E(F_{n,v}) \otimes \mathbf{Z}_p \\ Z_{\infty,s} &= Z_\infty / Z_{\infty,f} \end{aligned}$$

where we regard $Z_{\infty,f}$ as a Λ-submodule of Z_∞ via the Kummer map. Suppose we are given some $z \in H^1_{\mathrm{Iw}}(F_\Sigma/F_\infty, T_p(A))$ whose image $\mathcal{L}_z \in Z_{\infty,s}$ actually lands in $J^r Z_{\infty,s}$ with $r > 0$, say $\mathcal{L}_z = (\gamma - 1)^r y$ for some choice of topological generator $\gamma \in \Gamma$ and some $y \in Z_{\infty,s}$. Let y_0 denote the image of y in $H^1(F_p, T_p(A))/(A(F_p) \otimes \mathbf{Z}_p)$ and define

$$\lambda_z^{(r)} : A^\vee(F_p) \otimes \mathbf{Q}_p \ \to \ W_r$$

by $\lambda_z^{(r)}(a) = (y_0, a) \cdot (\gamma - 1)^r$, where $(\ ,\ )$ is the local Tate pairing.

Theorem 4.5. *With notation and definitions as above, let z_0 be the image of z in $H^1(F, T_p(A))$. Then $z_0 \in S_p^{(r)}(A/F)$ and for any $c \in S_p^{(r)}(A^\vee/F)$ we have*

$$h^{(r)}(z_0, c) = \lambda_z^{(r)}(c_p)$$

where c_p is the image of c in $A^\vee(F_p) \otimes \mathbf{Q}_p$.

Proof. Fix some positive integer k. First note that our assumption that all finite primes of Σ are finitely decomposed in F_∞ implies that z is unramified away from p, by Corollary B.3.5 of [16]. Hence, if $z(k)$ denotes the image of z in $\varprojlim H^1(F_n, A[p^k])$ (the limit being over n), we have $z(k) \in H^1_{\mathcal{F}^{\mathrm{rel}}}(F, S_{\mathrm{Iw}})$ where $S = A[p^k]$, $\mathcal{F}$ is the Selmer structure obtained by propagating the Selmer structure of Definition 3.2 through the injection $S_{\mathrm{Iw}} \ \to \ S_K$, and the notation $\mathcal{F}^{\mathrm{rel}}$ has the same meaning as in Section 2. We claim that the image of $z(k)$ in $H^1_{/\mathcal{F}}(F, S_{\mathrm{Iw}})$, which we shall denote $\mathcal{L}_z(k)$, is divisible by $(\gamma - 1)^r$. Indeed, it suffices to show that the natural map $Z_\infty \ \to \ H^1(F_p, S_{\mathrm{Iw}})$ takes $Z_{\infty,f}$ into $H^1_{\mathcal{F}}(F_p, S_{\mathrm{Iw}})$, so that we have a well-defined map $Z_{\infty,s} \ \to \ H^1_{/\mathcal{F}}(F, S_{\mathrm{Iw}})$. By Tate local duality, this is equivalent to the condition that the natural map

$$H^1(F_p, T_\infty) \ \to \ \varinjlim \oplus_{v|p} H^1(F_{n,v}, A^\vee[p^\infty])$$

takes $H^1_{\mathcal{F}^\vee}(F_p, T_\infty)$ into the image of $\varinjlim \oplus_{v|p}(A(F_{n,v}) \otimes \mathbf{Q}_p/\mathbf{Z}_p)$ under the Kummer map, where $T = A^\vee[p^k]$ and $\mathcal{F}^\vee$ is the Selmer structure of Definition 3.2. This claim now follows by replacing A by $A^\vee$ in Propositions 3.4 and 3.5 (strictly speaking, these propositions state that there is a natural map on global Selmer groups $H^1_{\mathcal{F}^\vee}(F, T_\infty) \to \mathrm{Sel}_{p^\infty}(A^\vee/F_\infty)$, but the proofs proceed by showing that the isomorphisms of local cohomology induced by Shapiro's lemma take the local conditions defining the left hand side into the local conditions defining the right hand side). We have now shown that the order of vanishing of $\mathcal{L}_z(k)$ is at least r, and so appealing to Theorem 2.5 we see that $z_0(k)$, the image of $z(k)$ under

$$H^1(F, S_{\mathrm{Iw}}) \to H^1(F, A[p^k]) \to H^1(F_\infty, A[p^k])[J],$$

lies in the submodule $Y_k^{(r)}$ defined at the beginning of this section. Passing to the limit over k we have $z_0 \in Y_\infty^{(r)}$, and therefore $z_0 \in S_p^{(r)}(A/F)$.

Now fix some $c \in Y_\infty^{\vee(r)}$ (the module defined in the same way as $Y_\infty^{(r)}$, but with A and $\mathcal{F}$ replaced by $A^\vee$ and $\mathcal{F}^\vee$). Passing to the limit in Theorem 2.5 we have the equality $h^{(r)}(z_0, c) = \lambda_z^{(r)}(c_p)$ in J^r/J^{r+1}, and extending by $\mathbf{Q}_p$-linearity proves the same result for $c \in S_p^{(r)}(A^\vee/F)$. □

In the special case where $S_p^{(1)}(A/F)$ is one-dimensional and $S_p^{(\infty)}(A/F)$ is trivial, the above theorem may be regarded as a p-adic, cohomological formulation of the Birch and Swinnerton-Dyer conjecture. In this situation $\exists\ \delta \geq 1$ such that

$$\dim_{\mathbf{Q}_p} S_p^{(r)}(A/F) = \begin{cases} 1 & r \leq \delta \\ 0 & r > \delta. \end{cases}$$

If $z_0 \neq 0$, the left hand side of the equality of the theorem can then be interpreted as a regulator term. By the theorem, $\mathcal{L}_z$ must vanish to order δ, and the right hand side is like the value of the δ^{th}-derivative. This interpretation breaks down when the dimension of $S_p^{(1)}(A/F)$ is greater than one, since the formula only allows one to compute the heights of elements against some fixed element z_0, and not all pairwise heights in a basis.

Of course this is only interesting if one can construct an element z for which we are somehow justified in calling $\mathcal{L}_z$ a p-adic L-function, and there are essentially two cases where this is understood: when $A/\mathbf{Q}$ is an elliptic curve, Kato has constructed such an element for which $\mathcal{L}_z$ is related to the Mazur–Swinnerton-Dyer p-adic L-function of E, and when A is a CM elliptic curve the Euler system of elliptic units is related, by work of Yager, to the two-variable p-adic L-function constructed by Katz. For applications of Theorem 4.5 in these special cases, see [1] for the elliptic unit case and [14, 15] for the case of Kato's Euler system.

References

[1] A. Agboola and B. Howard. Anticyclotomic Iwasawa theory of CM elliptic curves. *preprint*, 2003.

[2] M. Bertolini. Selmer groups and Heegner points in anticyclotomic $\mathbf{Z}_p$-extensions. *Compositio Mathematica*, 99:153–182, 1995.

[3] M. Bertolini and H. Darmon. Derived p-adic heights. *American Journal of Mathematics*, 117(6):1517–1554, 1995.

[4] J. Coates and R. Greenberg. Kummer theory for abelian varieties over local fields. *Invent. Math*, 124:129–174, 1996.

[5] C. Cornut. Mazur's conjecture on higher Heegner points. *Invent. Math*, 148:495–523, 2002.

[6] M. Flach. A generalisation of the Cassels-Tate pairing. *J. Reine Angew. Math.*, 412:113–127, 1990.
[7] R. Greenberg. Iwasawa theory for p-adic representations. In *Algebraic Number Theory*, volume 17 of *Adv. stud. in pure math.* Princeton University Press, 1989.
[8] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Inventiones Math.*, 18:183–266, 1972.
[9] B. Mazur and K. Rubin. Kolyvagin systems. *preprint*, 2002.
[10] B. Mazur and J. Tate. Canonical height pairings via biextensions. In M. Artin and J. Tate, editors, *Arithmetic and geometry*, volume 1, pages 195–238. Birkhäuser, Boston, 1983.
[11] J. Nekovář. Selmer complexes. Unpublished manuscript.
[12] B. Perrin-Riou. Théorie d'Iwasawa et hauteurs p-adiques. *Invent. Math.*, 109:137–185, 1992.
[13] B. Perrin-Riou. *p-adic L-functions and p-adic Representations*. American Mathematical Society, 2000.
[14] K. Rubin. Abelian varieties, p-adic heights and derivatives. In *Algebra and Number Theory*. Walter de Gruyter and Co., 1994.
[15] K. Rubin. Euler systems and modular elliptic curves. In *Galois Representations in Arithmetic Algebraic Geometry*, London Math. Soc. Lecture Notes 254, pages 351–367. Cambridge Univ. Press, 1998.
[16] K. Rubin. *Euler Systems*. Princeton University Press, 2000.

Department of Mathematics, Stanford University, Stanford, CA, 94305
Current address: Department of Mathematics, Harvard University, Cambridge, MA, 02138